

DEC 22 2015

Daniel J. Bradley, Clerk of Court

SealedPublic and unofficial staff access
to this instrument are
prohibited by court order.UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA

v.

CHRISTOPHER CORREA

Criminal No.

H15-679**INFORMATION**

THE UNITED STATES ATTORNEY CHARGES:

Introduction

At all times material to this Information:

1. The Houston Astros were a Major League Baseball team whose operations were primarily based within the Southern District of Texas. They were owned and managed by Houston Astros, LLC.
2. The St. Louis Cardinals were also a Major League Baseball team. They were owned and managed by St. Louis Cardinals, LLC.
3. The Astros and the Cardinals, like other teams, measured and analyzed in-game activities to gain advantages that may not have been apparent to their competitors.
4. Defendant Christopher Correa was, from 2009 to July 2015, employed by the St. Louis Cardinals. In 2013, he became the Cardinals' Director of Baseball Development, where he provided analytical support to all areas of the Cardinals' baseball operations.
5. Until late 2011, Victims A and B were both employed by the St. Louis Cardinals, and like Correa, they focused on analytics. After that, they joined the Astros.
6. The Astros operated an email system for their employees. The Astros also operated a private online database called Ground Control. Both systems were maintained on

computers located in the Southern District of Texas that were used in (and affected) interstate commerce and communication. The Astros used Ground Control to house a wide variety of confidential data, including scouting reports, statistics, and contract information, all to improve the team's scouting, communication, and decision-making for every baseball-related decision. Victims A and B, as well as other Astros employees, were assigned password-protected accounts by which they could access Ground Control and their Astros e-mail.

7. From no later than March 2013 to the end of June 2014, defendant Christopher Correa accessed the computers of the Houston Astros without authorization. In particular, he accessed Victim A's e-mail account and the Ground Control accounts of Victim A, Victim B, and other Astros employees.

8. Correa illegally accessed the Astros' computers in the following way: In December 2011, as Victim A prepared to leave the St. Louis Cardinals and join the Houston Astros, he was directed to turn over his Cardinals-owned laptop to Correa – along with the laptop's password. When Victim A joined the Astros, he re-used a similar (albeit obscure) password for his Astros' e-mail and Ground Control accounts. No later than March 2013, Correa began accessing Victim A's Ground Control and Astros' e-mail accounts using this variation of the password to Victim A's Cardinals laptop.

9. On March 24, 2013, Correa accessed Victim A's Ground Control account, and downloaded an Excel file of the Astros' scouting list of every player eligible for that year's draft, and how each Astros scout ranked them. He also viewed, among other things, the following confidential information:

- Scouting weekly digest page, which listed stats and notes on recent performance and injuries for top prospects whom the Astros were considering drafting, as well as a regional scout's evaluations of his prospects' estimated peak rise, and the bonus he proposed be offered;

- Scouting crosscheck page, which listed prospects seen by cross-checkers (higher level scouts – as players are more likely to be drafted, more scouting resources are devoted to evaluating them) and scouting page;
- Astros main draft page, as well as subsets of players such as college hitters, high school pitchers, etc. whom the Astros were considering drafting, ranked by analytics, and the bonus proposed to be offered;
- Multiple webpages about the St. Louis Cardinals including the Astros' notes page, and the Astros' evaluations of Cardinals prospects;
- Astros' notes of trade discussions, filtered to focus: (a) on notes entered by the Astros' General Manager (GM), Assistant GM, Director of Amateur Scouting; (b) all Astros' trade notes for the past year; and (c) notes of the Astros' trade discussions with the Cardinals.

10. In the early morning of June 8, 2013, before the start of Day 3 of Major League Baseball's 2013 Amateur Draft, Correa again accessed Victim A's Ground Control account and viewed the Astros' draft page, filtering results to only view players who had not yet been drafted. He also viewed Astros draft pages for Player G, whom the Astros drafted later that day, and Player H, who was drafted by another team. He also viewed the Astros' information on Players I, J, and K, three players whom the Cardinals had drafted the day before.

11. On July 31, 2013, before Major League Baseball's July 31, 2013 Non-Wavier Trade Deadline, Correa again accessed Victim A's Ground Control account and viewed the Astros' notes on its trade discussions with other teams.

12. Around March 9, 2014, the Houston Chronicle published an in-depth article about Ground Control. This article was picked up by other media outlets across the country.

13. The Astros reacted by implementing several security precautions. The team changed Ground Control's website address (URL). It also required all Ground Control users to change their passwords to more complex passwords the next time they logged in. Concerned that (a) some users would not log into Ground Control soon enough to change their password,

and that (b) some of those users' existing passwords might have been guessed, the team also reset all Ground Control passwords to a more complex default password, and e-mailed the new default password and the new URL to all Ground Control users.

14. On the evening of March 10, 2014, shortly after the Chronicle's article was carried nationwide, defendant Correa again accessed Victim A's Astros e-mail account without authorization. There, he found the e-mails that contained Ground Control's new URL and the newly reset password.

15. A few minutes later, Correa used the information he obtained from Victim A's e-mail account to access Victim B's Ground Control account without authorization. There, Correa viewed 118 pages containing confidential information such as:

- Notes of the Astros' trade discussions with other MLB teams;
- Lists ranking the players whom Astros scouts desired in the upcoming amateur draft, in order of desirability;
- Summaries of evaluations written by Astros scouts of amateur players whom the Astros were considering drafting;
- The Astros' Amateur Draft Board for 2014 (which was not yet completed), and then for 2013 (which was);
- Summaries of the college pitchers and hitters whom the Astros' analytics department regarded as the top performers; and
- Evaluations written by Astros scouts of international players whom the Astros were considering offering contracts.

COUNTS 1 TO 5
Unauthorized Access of a Protected Computer

1. The allegations set forth in the Introduction are re-alleged and incorporated by reference as if set forth in full.

2. On or about the dates listed below, in the Southern District of Texas and elsewhere, defendant

CHRISTOPHER CORREA

intentionally accessed a computer without authorization, and thereby obtained information from a computer that was used in and affecting interstate and foreign commerce and communication, and the value of the information obtained exceeded \$5,000, in violation of 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(iii).

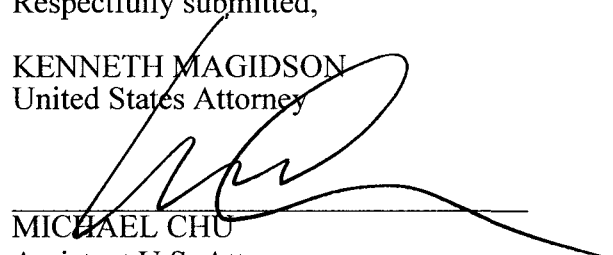
Ct	Date	Description
1	March 24, 2013	Accessed Victim A's Ground Control account without authorization, which was maintained on a computer located in the Southern District of Texas
2	June 8, 2013	Accessed Victim A's Ground Control account without authorization, which was maintained on a computer located in the Southern District of Texas
3	July 31, 2013	Accessed Victim A's Ground Control account without authorization, which was maintained on a computer located in the Southern District of Texas
4	March 10, 2014	Accessed Victim A's e-mail account without authorization, which was maintained on a computer located in the Southern District of Texas
5	March 10, 2014	Accessed Victim B's Ground Control account without authorization, which was maintained on a computer located in the Southern District of Texas

All in violation of Title 18, United States Code, Sections 1030(a)(2)(C) & (c)(2)(B)(iii).

Respectfully submitted,

KENNETH MAGIDSON
United States Attorney

By:


MICHAEL CHU
Assistant U.S. Attorney